Configurar Alta Disponibilidade de FTD Usando FDM

Contents

Introdução

Este documento descreve como configurar um par de HA (High Availability, alta disponibilidade) ativo/standby de FTD (Secure Firewall Threat Defense, defesa contra ameaças de firewall) gerenciado localmente.

Pré-requisitos

Requisitos

Recomenda-se ter conhecimento destes tópicos:

- Configuração inicial do Cisco Secure Firewall Threat Defense via GUI e/ou shell.

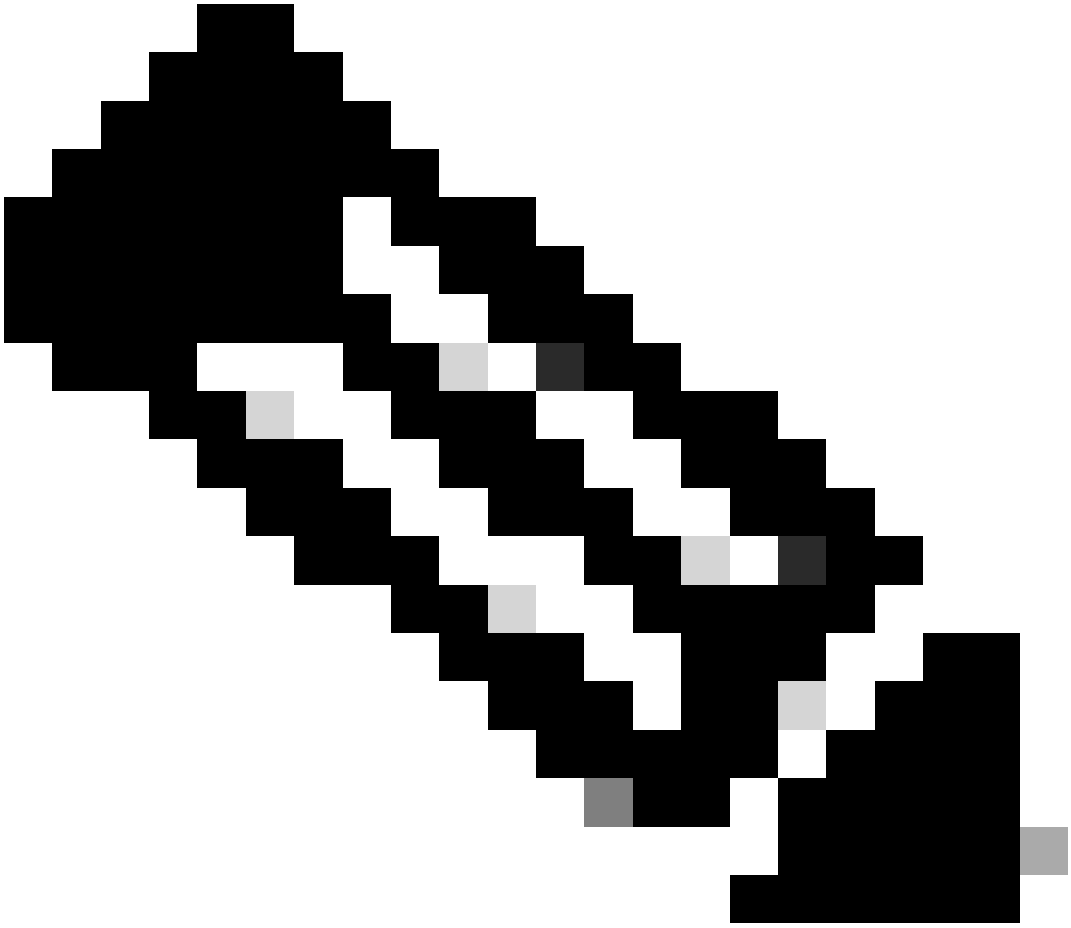
Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

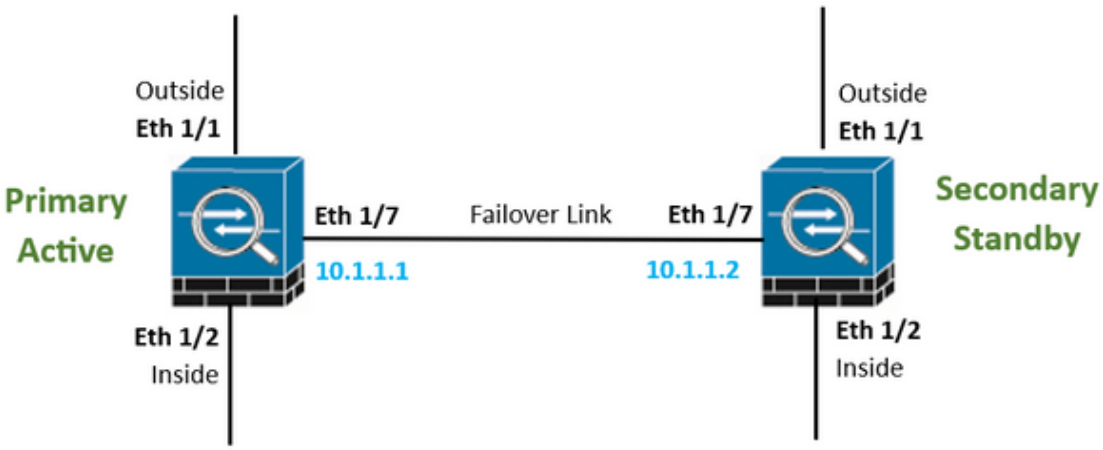
- FPR2110 versão 7.2.5 gerenciado localmente pelo Firepower Device Manager (FDM)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Topologia de rede



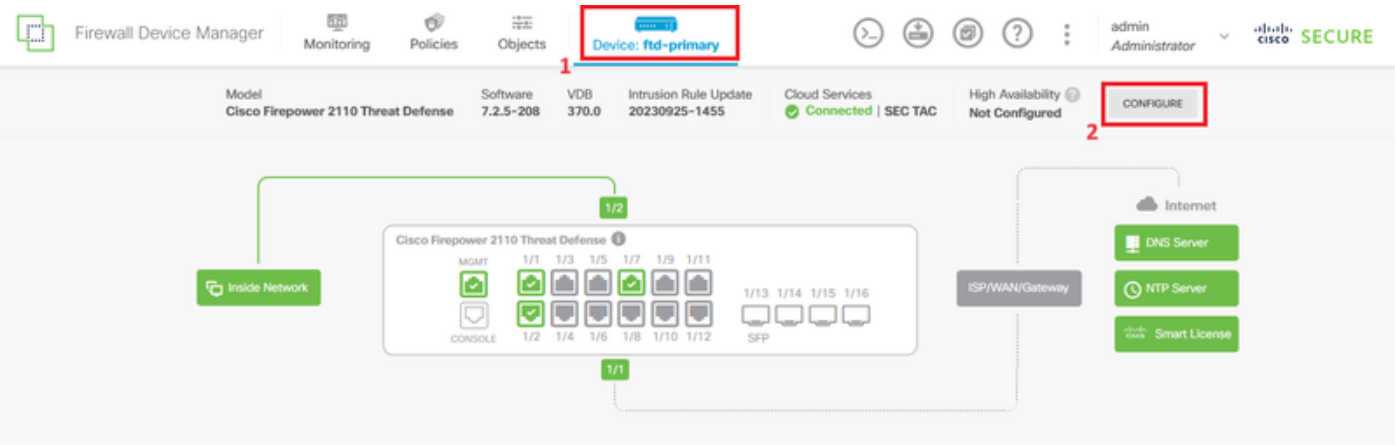
Observação: o exemplo descrito neste documento é um dos vários projetos de rede recomendados. Consulte o guia de configuração Como evitar failover interrompido e links de dados para obter mais opções.



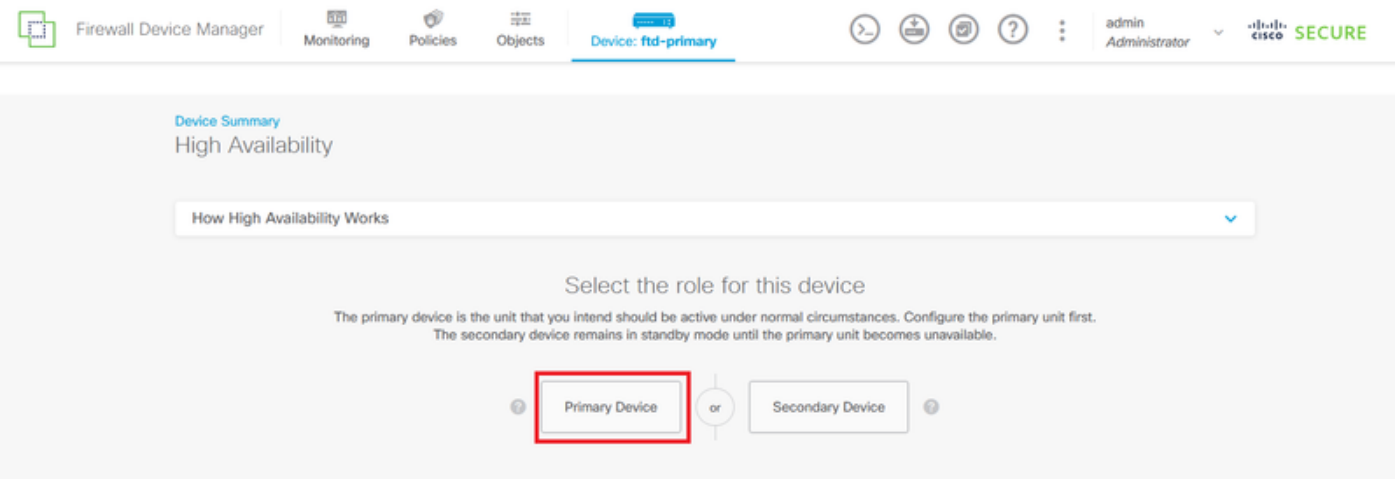
Configurar

Configurar a Unidade Principal para Alta Disponibilidade

Etapa 1. Clique em Device e pressione o botão Configure no canto superior direito, ao lado do status High Availability (Alta disponibilidade).



Etapa 2. Na página High Availability (Alta disponibilidade), clique na caixa Primary Device.



Etapa 3. Configure as propriedades do Link de Failover.

Selecione a interface conectada diretamente ao firewall secundário e defina o endereço IP primário e secundário, bem como a sub-rede Netmask.

Marque a caixa de seleção Usar a mesma interface que o link de failover para o link de failover stateful.

Desmarque a caixa Chave de criptografia IPSec e clique em Ativar HA para salvar as alterações.

I have configuration of peer device in clipboard PASTE FROM CLIPBOARD

FAILOVER LINK

Interface

unnamed (Ethernet1/7)

Type

IPv4 IPv6

Primary IP

10.1.1.1

e.g. 192.168.10.1

Secondary IP

10.1.1.2

e.g. 192.168.10.2

Netmask

255.255.255.252

e.g. 255.255.255.0 or 24

STATEFUL FAILOVER LINK

Use the same interface as the Failover Link

Interface

unnamed (Ethernet1/7)

Type

IPv4 IPv6

Primary IP

10.1.1.1

e.g. 192.168.11.1

Secondary IP

10.1.1.2

e.g. 192.168.11.2

Netmask

255.255.255.252

e.g. 255.255.255.0 or 24

IPSec Encryption Key *(optional)*

For security purposes, the encryption key will not be included in the configuration copied to the clipboard when you activate HA.
You will need to manually enter the key when you configure HA on the peer device.

IMPORTANT

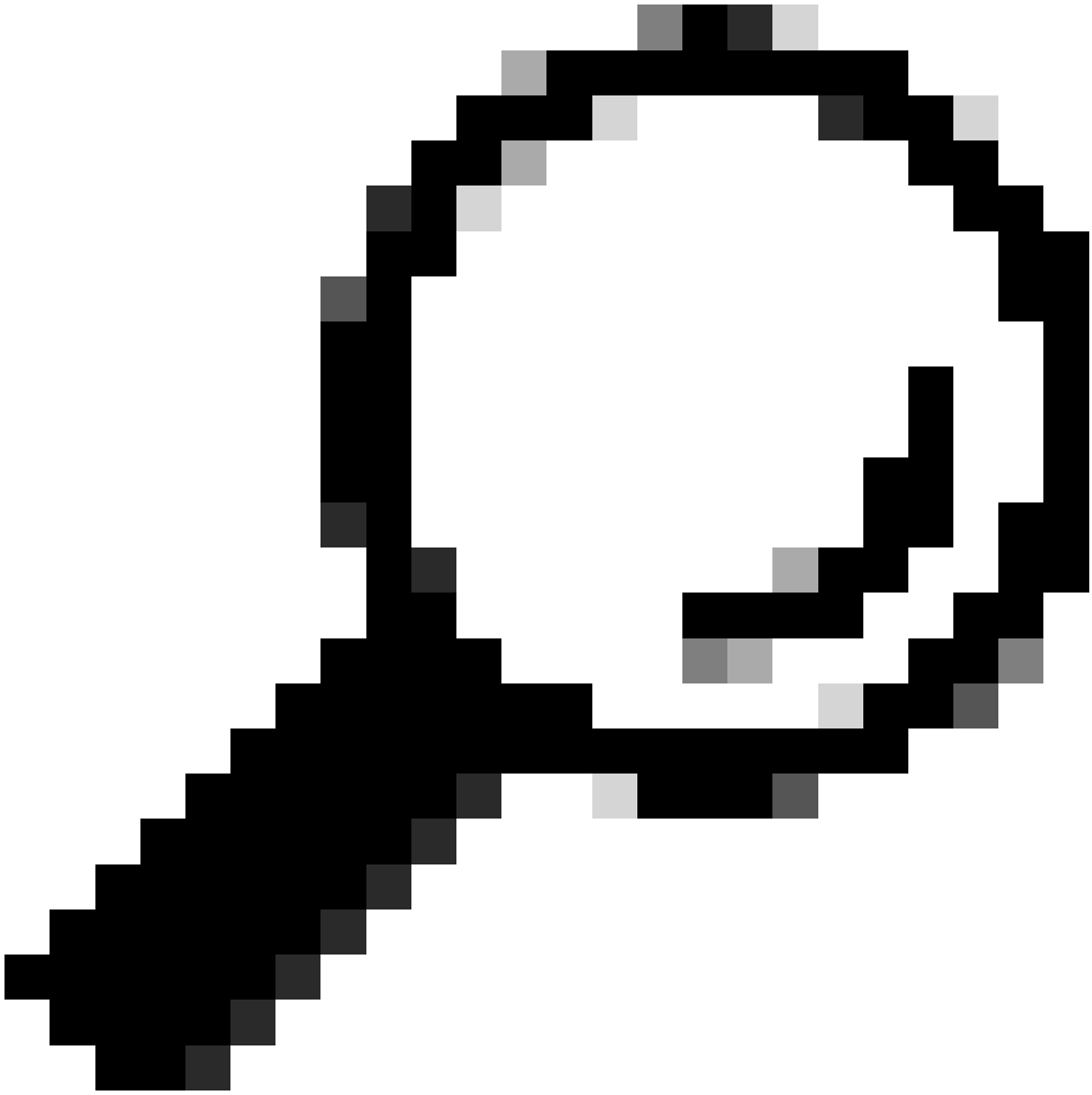
If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. Learn More

Before you activate HA, make sure both devices have the same Smart License and Cloud Region. Otherwise HA will not work.

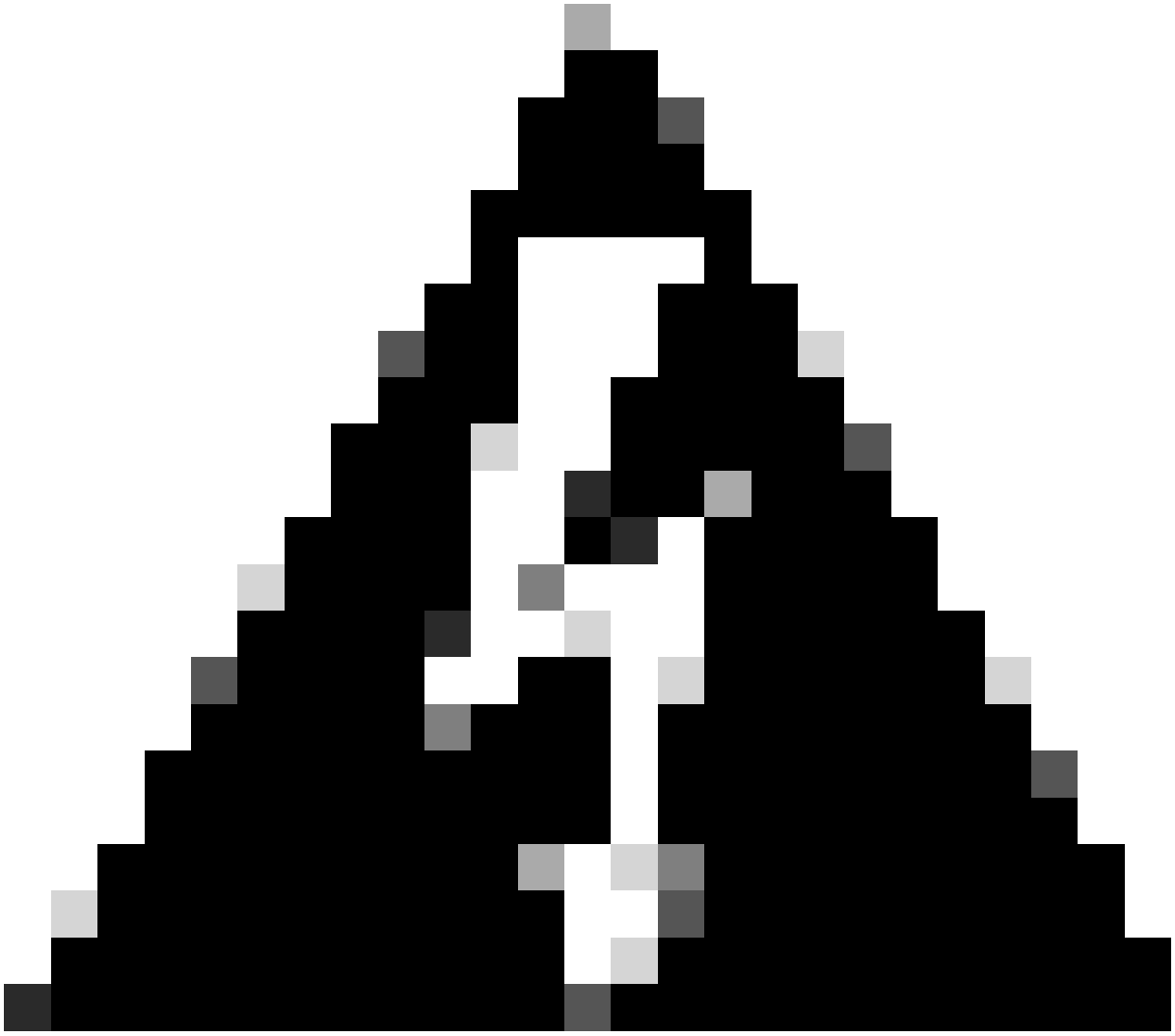
When you click Activate HA, these settings are automatically deployed to the device. The deployment might restart inspection engines, which can result in the momentary traffic loss. It might take a few minutes for deployment to finish.

Information is copied to the clipboard when deployment is done. You must allow the browser to access your clipboard for the copy to be successful.

ACTIVATE HA

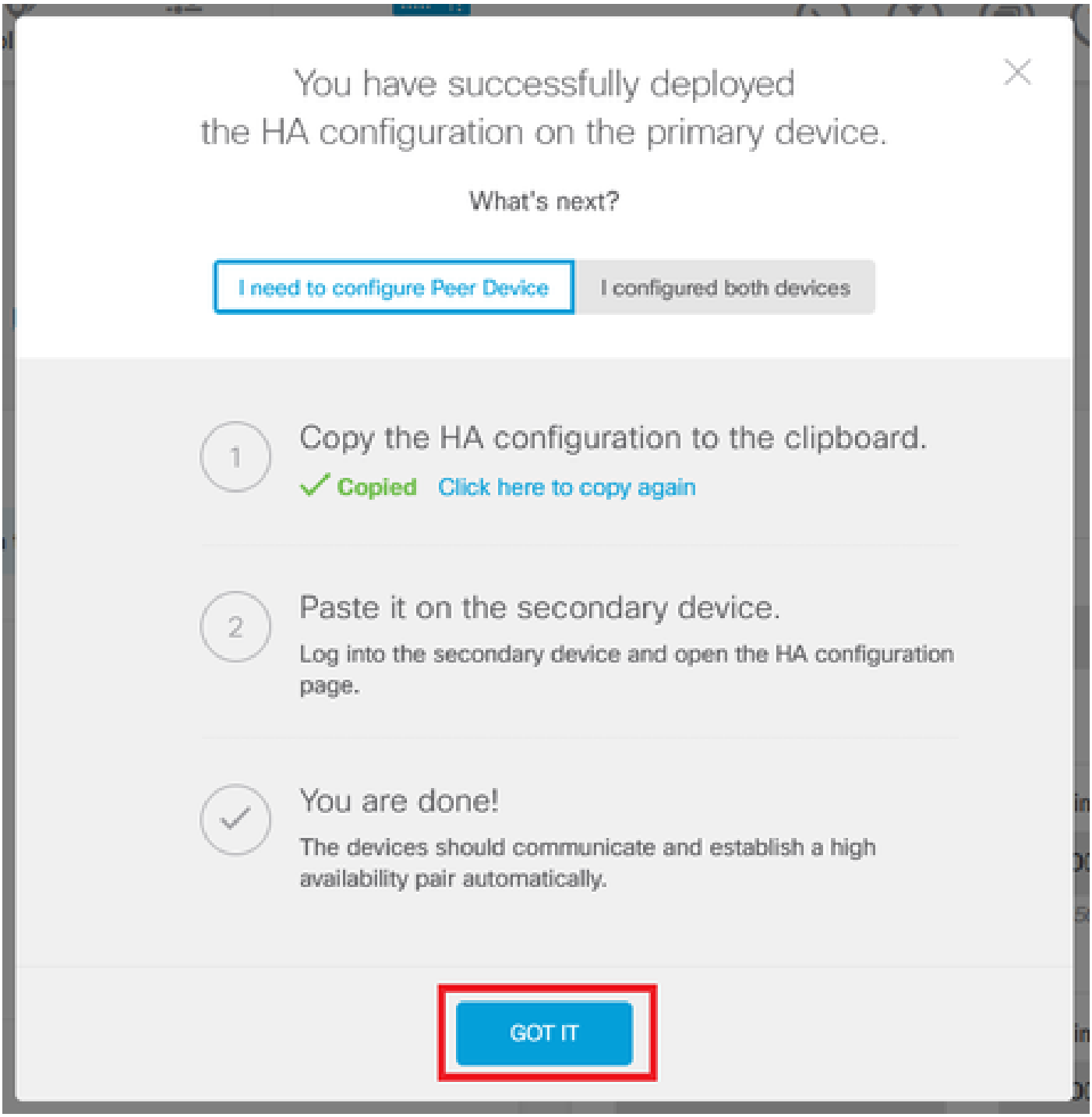


Dica: use uma sub-rede de máscara pequena, dedicada ao tráfego de failover somente para evitar violações de segurança e/ou problemas de rede o máximo possível.



Aviso: o sistema implanta imediatamente a configuração no dispositivo. Não é necessário iniciar um trabalho de implantação. Se você não vir uma mensagem informando que sua configuração foi salva e a implantação está em andamento, role para a parte superior da página para ver as mensagens de erro. A configuração também é copiada para a área de transferência. Você pode usar a cópia para configurar rapidamente a unidade secundária. Para maior segurança, a chave de criptografia (se você definir uma) não é incluída na cópia da área de transferência.

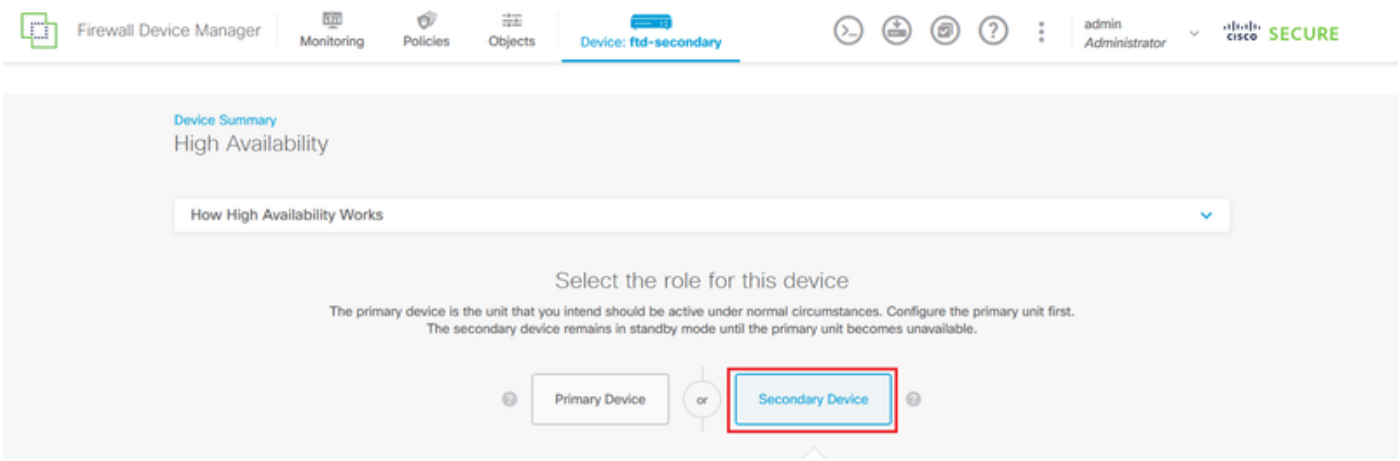
Etapa 4. Após a conclusão da configuração, você receberá uma mensagem explicando as próximas etapas. Depois de ler as informações, clique em Got It.



Configurar a unidade secundária para alta disponibilidade

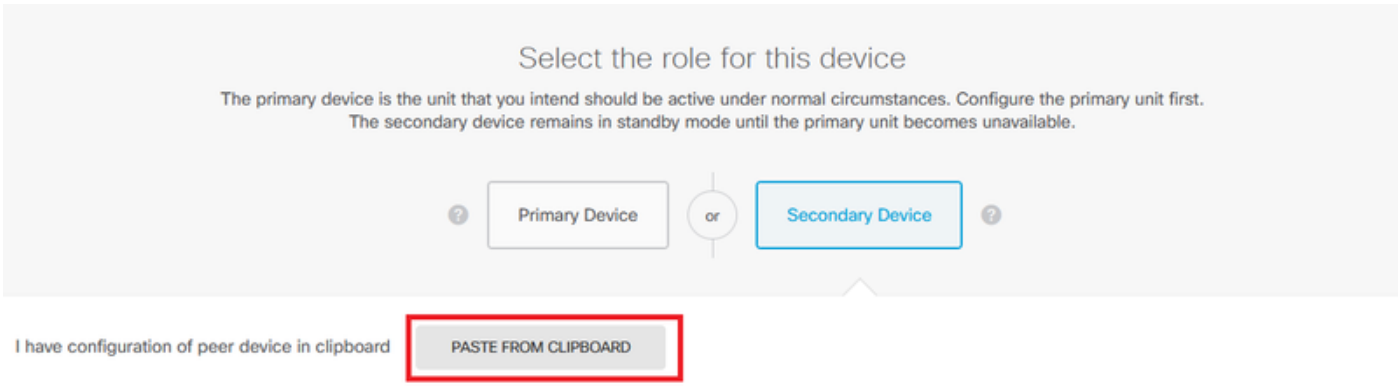
Etapa 1. Clique em Device e pressione o botão Configure no canto superior direito, ao lado do status High Availability (Alta disponibilidade).

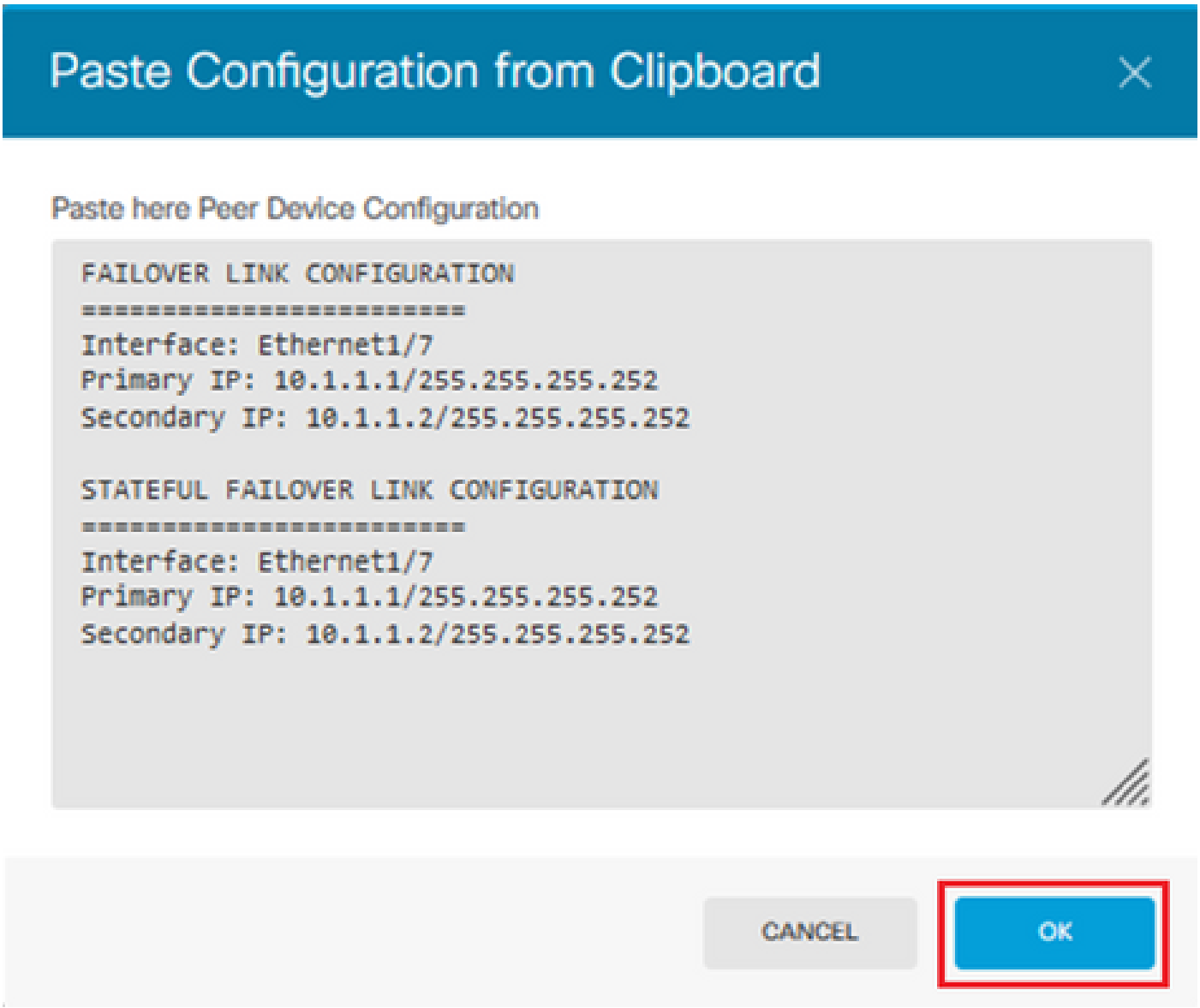
Etapa 2. Na página Alta disponibilidade, clique na caixa Dispositivo secundário.



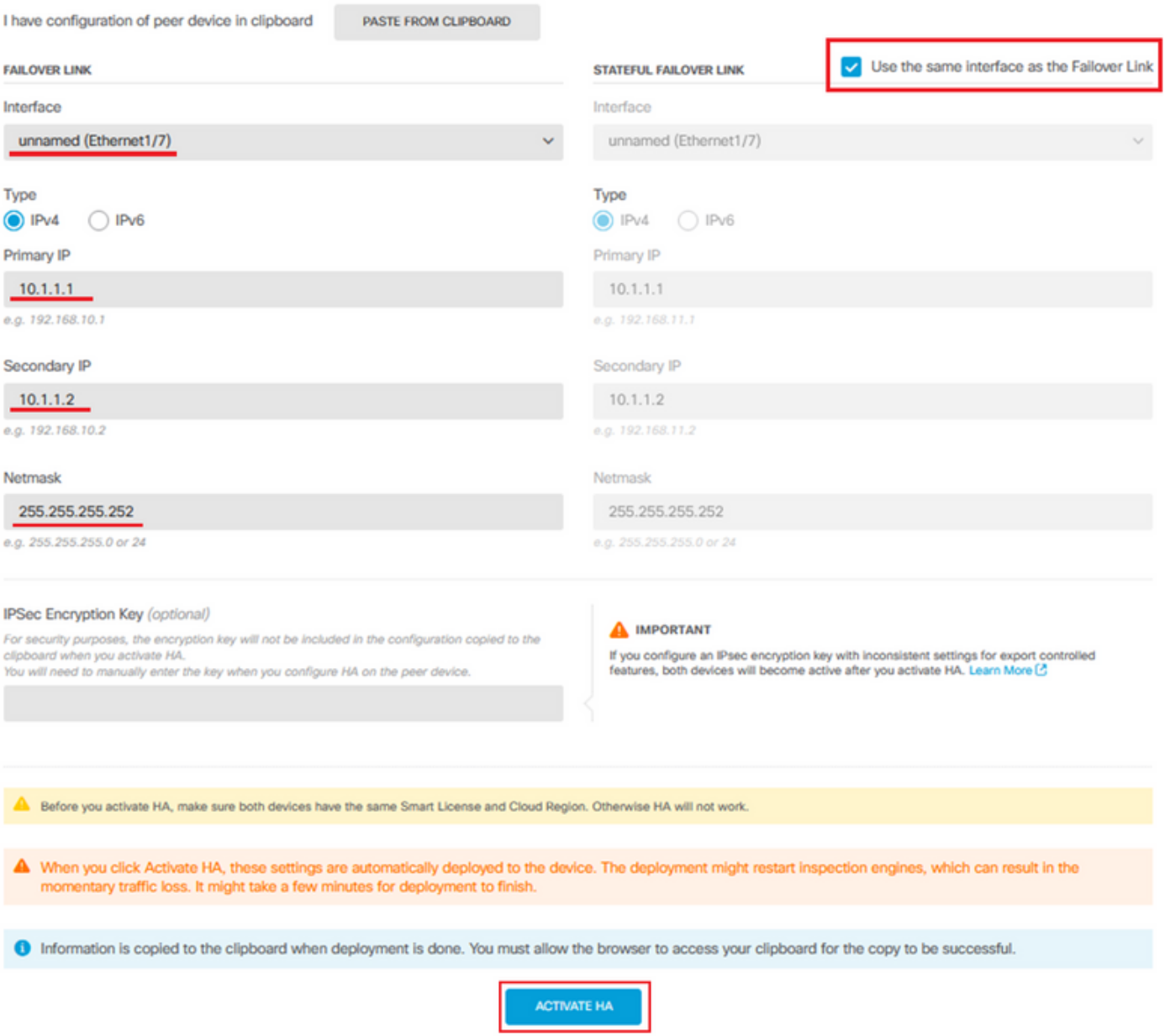
Etapa 3. Configure as propriedades do Link de Failover. Você pode colar as configurações armazenadas na área de transferência após configurar o FTD primário ou pode continuar manualmente.

Etapa 3.1. Para colar da área de transferência, basta clicar no botão Colar da área de transferência, colar na configuração (pressione as teclas Ctrl+v simultaneamente) e clicar em OK.

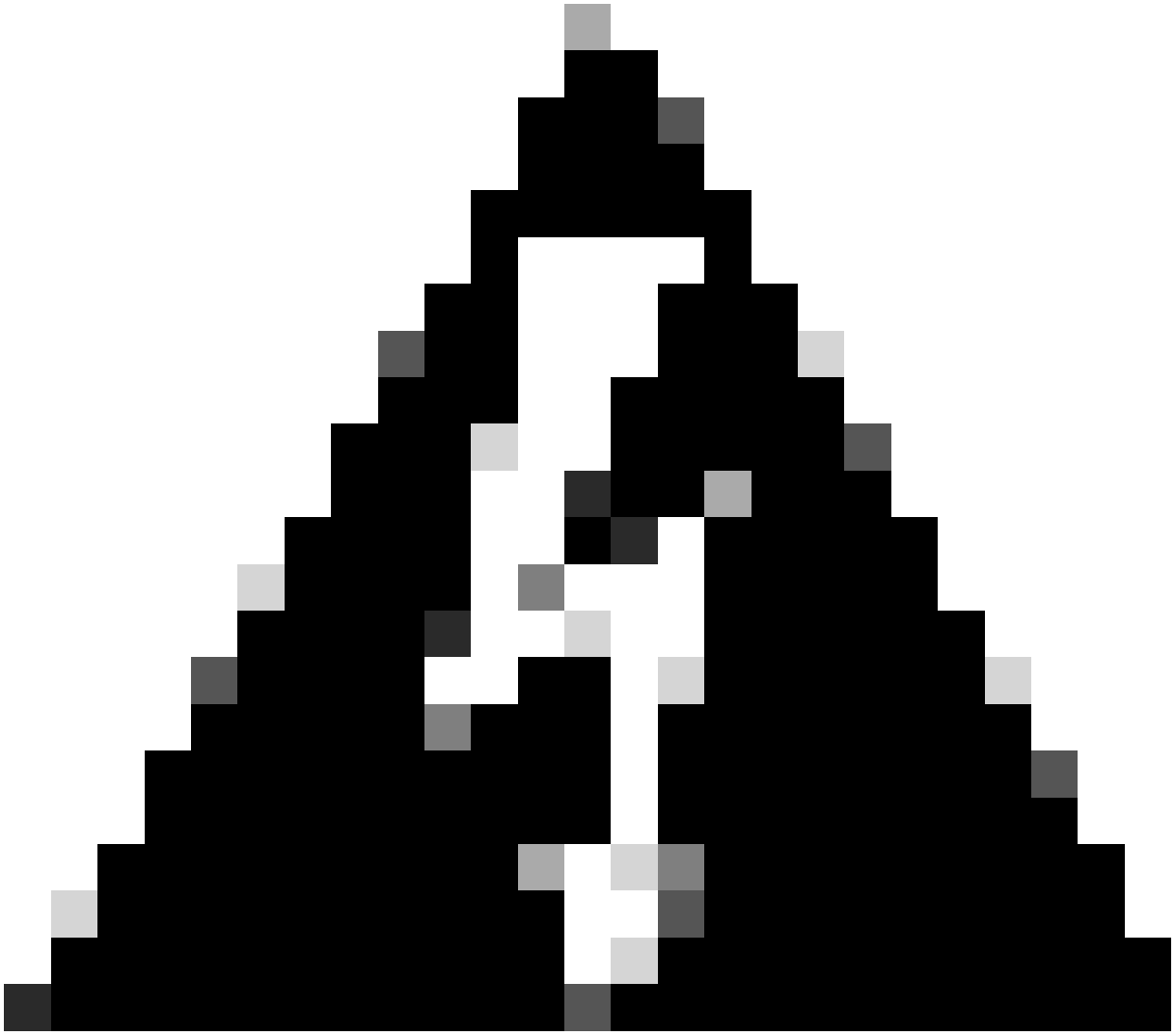




Etapa 3.2. Para continuar manualmente, selecione a interface conectada diretamente ao firewall secundário e defina o endereço IP primário e secundário, bem como a sub-rede Netmask. Marque a caixa de seleção Usar a mesma interface que o link de failover para o link de failover stateful.

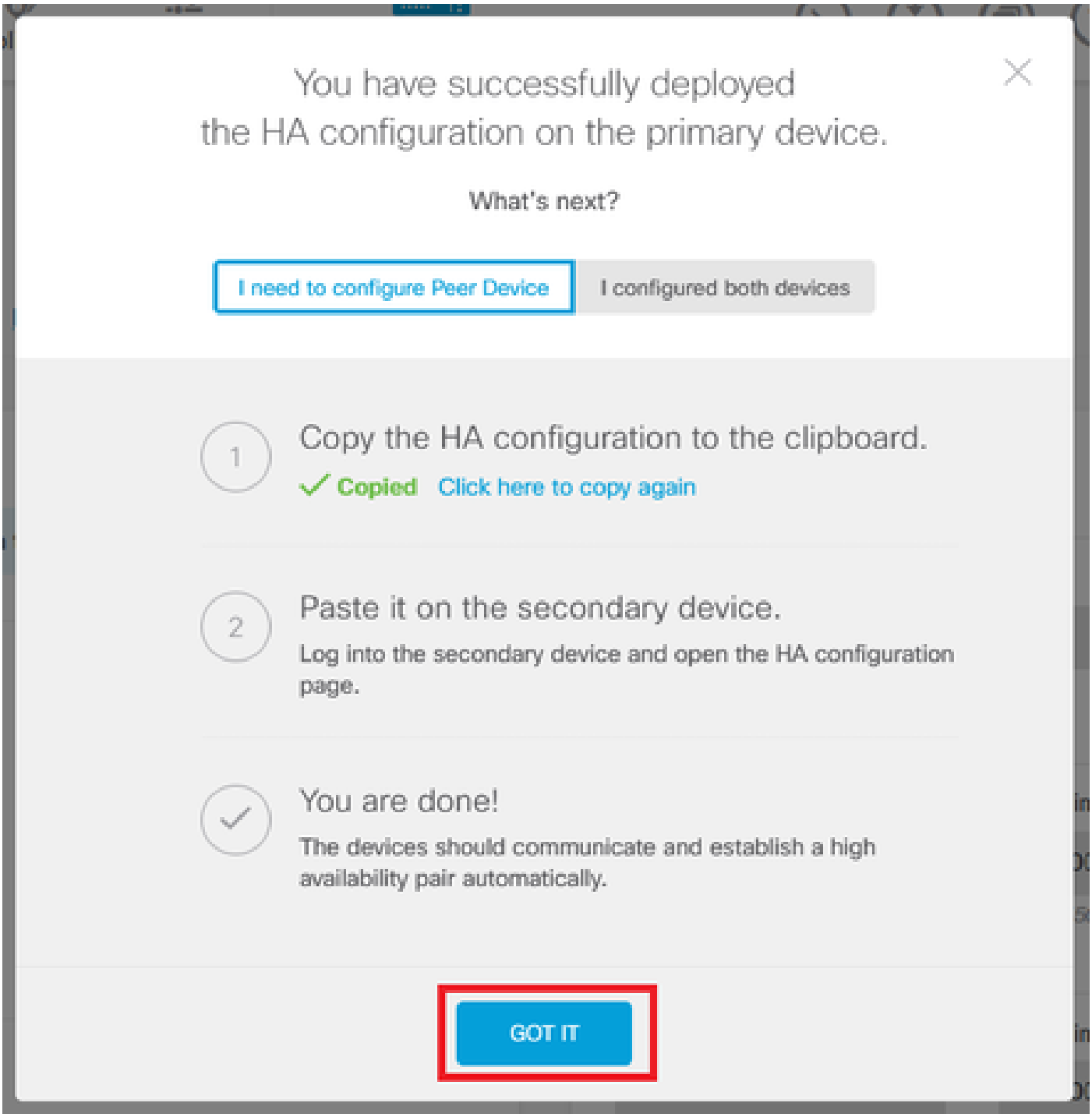


Etapa 4. Desmarque a caixa Chave de criptografia IPSec e clique em Ativar HA para salvar as alterações.



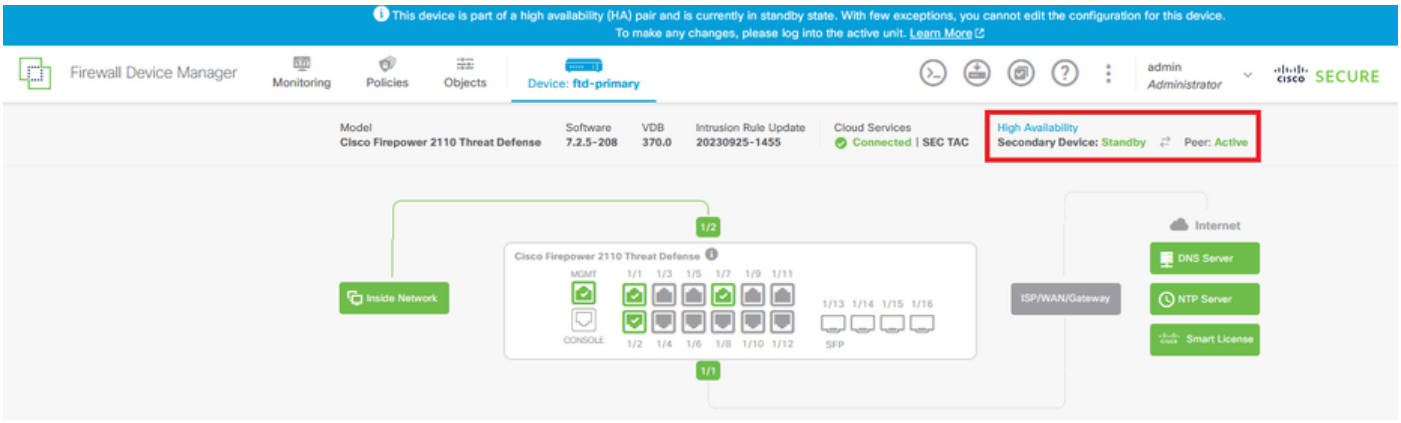
Aviso: o sistema implanta imediatamente a configuração no dispositivo. Não é necessário iniciar um trabalho de implantação. Se você não vir uma mensagem informando que sua configuração foi salva e a implantação está em andamento, role para a parte superior da página para ver as mensagens de erro.

Etapa 5. Após a conclusão da configuração, você receberá uma mensagem explicando as próximas etapas que devem ser executadas. Depois de ler as informações, clique em Got It.

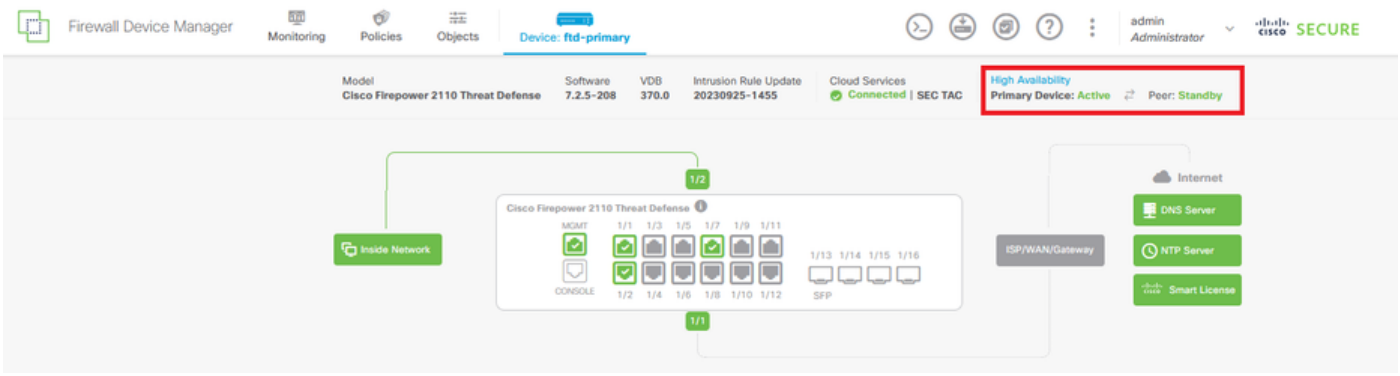


Verificar

- Nesse ponto, a maioria dos status do dispositivo indica que esse é o dispositivo secundário na página Alta disponibilidade. Se a junção com o dispositivo primário foi bem-sucedida, o dispositivo começa a sincronizar com o primário e, eventualmente, o modo é alterado para Standby e o peer para Ative.



- O FTD Principal também deve mostrar o status de Alta Disponibilidade, mas como Ativo e Par: Em Espera.



- Abra uma sessão SSH para o FTD principal e emita o comando show running-config failover para verificar a configuração.

```
> show running-config failover
failover
failover lan unit primary
failover lan interface failover-link Ethernet1/7
failover replication http
failover link failover-link Ethernet1/7
failover interface ip failover-link 10.1.1.1 255.255.255.252 standby 10.1.1.2
```

- Valide o status atual do dispositivo com o comando show failover state.

```
> show failover state

              State          Last Failure Reason      Date/Time
This host  -  Primary
              Active         None
Other host -  Secondary
              Standby Ready  None

====Configuration State===
====Communication State===
        Mac set

>
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.